TITLE: MULTI-AUTHENTICATION FOR A COMPUTING DEVICE CONNECTING TO A NETWORK
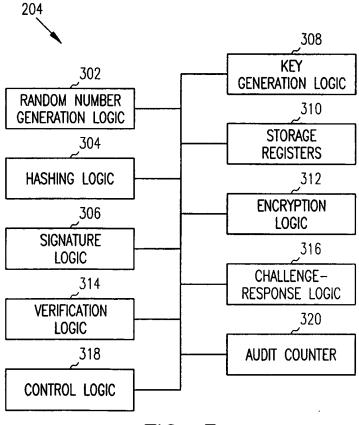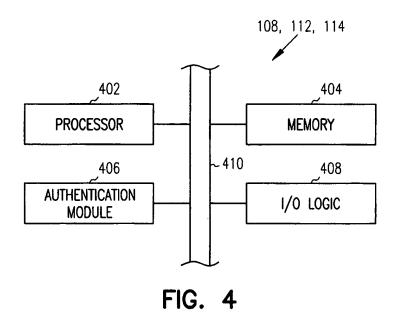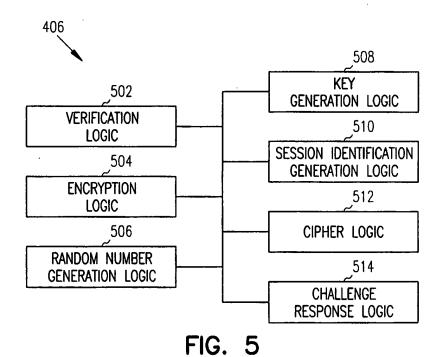INVENTORS NAME: Selim Aissi et al.
DOCKET NO.: 884.B30US1

1/11

FIG. 1

TITLE: MULTI-AUTHENTICATION FOR A COMPUTING DEVICE CONNECTING TO A NETWORK
INVENTORS NAME: Selim Aissi et al.
DOCKET NO.: 884.B30US1

2/11

102

202	208
PROCESSOR	MEMORY

~212

204	210
CRYPTOGRAPHIC PROCESSING MODULE	I/O LOGIC

206	214
COMMUNICATIONS PROCESSOR	MEMORY

FIG. 2

204

302	308
RANDOM NUMBER GENERATION LOGIC	KEY GENERATION LOGIC

304	310
HASHING LOGIC	STORAGE REGISTERS

306	312
SIGNATURE LOGIC	ENCRYPTION LOGIC

314	316
VERIFICATION LOGIC	CHALLENGE-RESPONSE LOGIC

318	320
CONTROL LOGIC	AUDIT COUNTER

FIG. 3

TITLE: MULTI-AUTHENTICATION FOR A COMPUTING DEVICE CONNECTING TO A NETWORK
INVENTORS NAME: Selim Aissi et al.
DOCKET NO.: 884.B30US1

3/11

108, 112, 114

402		404
PROCESSOR		MEMORY

~410

406		408
AUTHENTICATION MODULE		I/O LOGIC

FIG. 4

406

502		508
VERIFICATION LOGIC		KEY GENERATION LOGIC

504		510
ENCRYPTION LOGIC		SESSION IDENTIFICATION GENERATION LOGIC

506		512
RANDOM NUMBER GENERATION LOGIC		CIPHER LOGIC

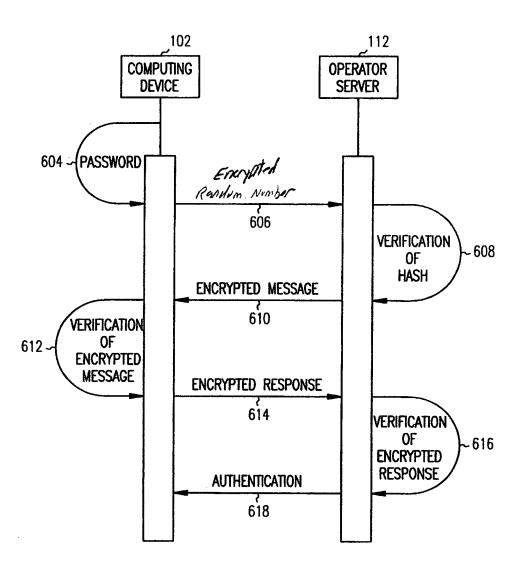|		514
		CHALLENGE RESPONSE LOGIC

FIG. 5

TITLE: MULTI-AUTHENTICATION FOR A COMPUTING DEVICE CONNECTING TO A NETWORK
INVENTORS NAME: Selim Aissi et al.
DOCKET NO.: 884.B30US1

4/11

102
COMPUTING
DEVICE

112
OPERATOR
SERVER

604 — PASSWORD

Encrypted
Random Number
606

VERIFICATION
OF
HASH
608

ENCRYPTED MESSAGE
610

612 — VERIFICATION
OF
ENCRYPTED
MESSAGE

ENCRYPTED RESPONSE
614

VERIFICATION
OF
ENCRYPTED
RESPONSE
616

AUTHENTICATION
618

FIG. 6

TITLE: MULTI-AUTHENTICATION FOR A COMPUTING DEVICE CONNECTING TO A NETWORK
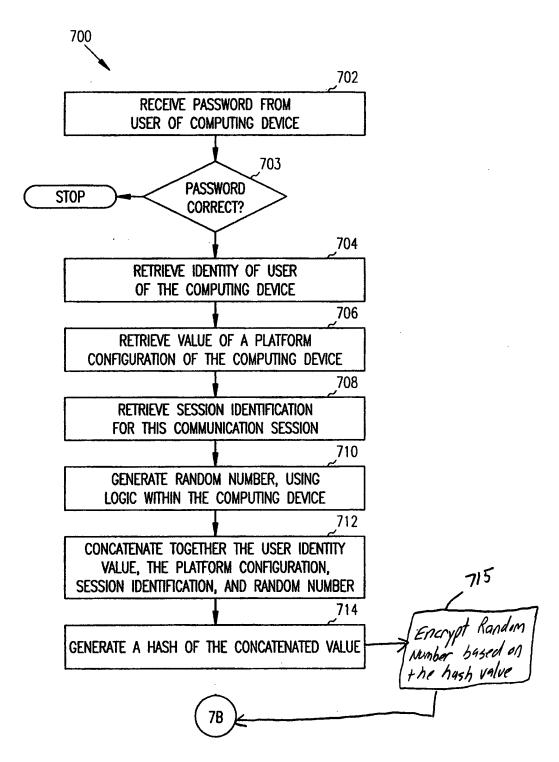INVENTORS NAME: Selim Aissi et al.
DOCKET NO.: 884.B30US1

5/11

700

702

RECEIVE PASSWORD FROM
USER OF COMPUTING DEVICE

703

PASSWORD
CORRECT?

STOP

704

RETRIEVE IDENTITY OF USER
OF THE COMPUTING DEVICE

706

RETRIEVE VALUE OF A PLATFORM
CONFIGURATION OF THE COMPUTING DEVICE

708

RETRIEVE SESSION IDENTIFICATION
FOR THIS COMMUNICATION SESSION

710

GENERATE RANDOM NUMBER, USING
LOGIC WITHIN THE COMPUTING DEVICE

712

CONCATENATE TOGETHER THE USER IDENTITY
VALUE, THE PLATFORM CONFIGURATION,
SESSION IDENTIFICATION, AND RANDOM NUMBER

714

GENERATE A HASH OF THE CONCATENATED VALUE

715

Encrypt Random
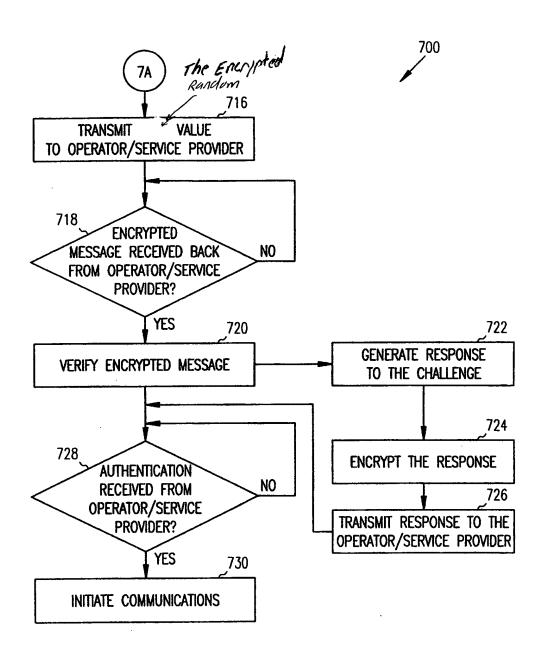Number based on
the hash value

7B

FIG. 7A

TITLE: MULTI-AUTHENTICATION FOR A COMPUTING DEVICE CONNECTING TO A NETWORK
INVENTORS NAME: Selim Aissi et al.
DOCKET NO.: 884.830US1

6/11
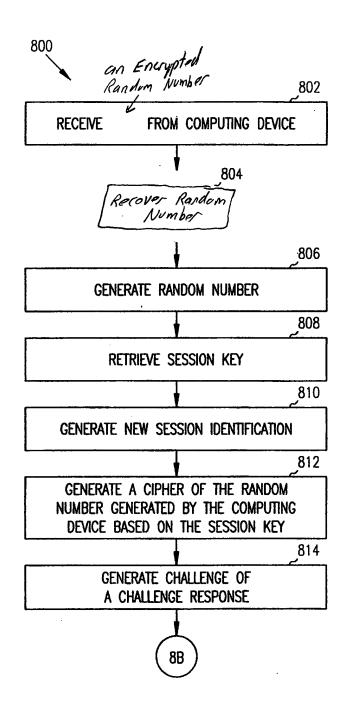
700

7A   The Encrypted Random

716

TRANSMIT VALUE
TO OPERATOR/SERVICE PROVIDER

718

ENCRYPTED
MESSAGE RECEIVED BACK
FROM OPERATOR/SERVICE
PROVIDER?   NO

YES

720
VERIFY ENCRYPTED MESSAGE

722
GENERATE RESPONSE
TO THE CHALLENGE

724
ENCRYPT THE RESPONSE

726
TRANSMIT RESPONSE TO THE
OPERATOR/SERVICE PROVIDER

728

AUTHENTICATION
RECEIVED FROM
OPERATOR/SERVICE
PROVIDER?   NO

YES

730
INITIATE COMMUNICATIONS

FIG. 7B

TITLE: MULTI-AUTHENTICATION FOR A COMPUTING DEVICE CONNECTING TO A NETWORK
INVENTORS NAME: Selim Aissi et al.
DOCKET NO.: 884.B30US1

7/11

800

an Encrypted Random Number

802

RECEIVE **FROM COMPUTING DEVICE**

804

Recover Random Number

806

GENERATE RANDOM NUMBER

808

RETRIEVE SESSION KEY

810

GENERATE NEW SESSION IDENTIFICATION

812

GENERATE A CIPHER OF THE RANDOM
NUMBER GENERATED BY THE COMPUTING
DEVICE BASED ON THE SESSION KEY

814

GENERATE CHALLENGE OF
A CHALLENGE RESPONSE

8B

FIG. 8A

TITLE: MULTI-AUTHENTICATION FOR A COMPUTING DEVICE CONNECTING TO A NETWORK
INVENTORS NAME: Selim Aissi et al.
DOCKET NO.: 884.830US1

8/11
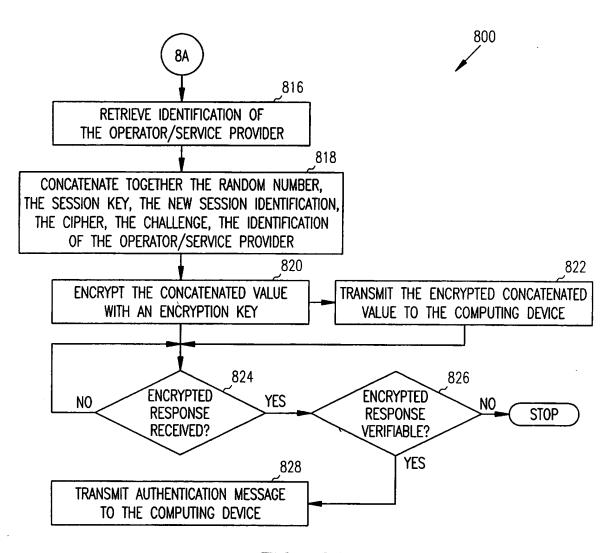
800

8A

RETRIEVE IDENTIFICATION OF
THE OPERATOR/SERVICE PROVIDER
816

CONCATENATE TOGETHER THE RANDOM NUMBER,
THE SESSION KEY, THE NEW SESSION IDENTIFICATION,
THE CIPHER, THE CHALLENGE, THE IDENTIFICATION
OF THE OPERATOR/SERVICE PROVIDER
818

ENCRYPT THE CONCATENATED VALUE
WITH AN ENCRYPTION KEY
820

TRANSMIT THE ENCRYPTED CONCATENATED
VALUE TO THE COMPUTING DEVICE
822

ENCRYPTED
RESPONSE
RECEIVED?
824
NO
YES

ENCRYPTED
RESPONSE
VERIFIABLE?
826
NO
STOP

YES

TRANSMIT AUTHENTICATION MESSAGE
TO THE COMPUTING DEVICE
828

FIG. 8B

TITLE: MULTI-AUTHENTICATION FOR A COMPUTING DEVICE CONNECTING TO A NETWORK
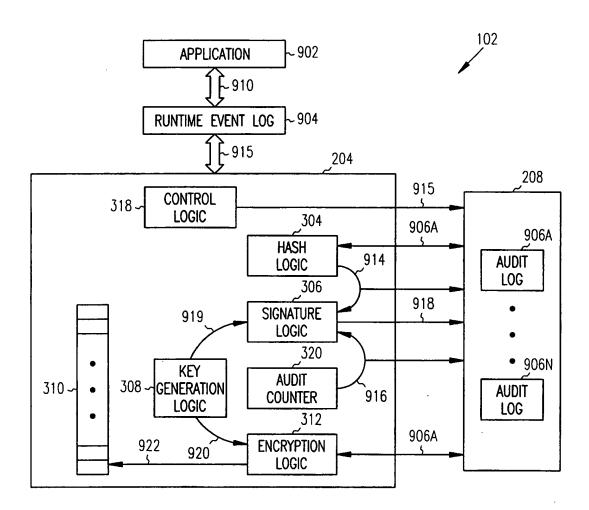INVENTORS NAME: Selim Aissi et al.
DOCKET NO.: 884.B30US1

9/11

FIG. 9

FIG. 10A

TITLE: MULTI-AUTHENTICATION FOR A COMPUTING DEVICE CONNECTING TO A NETWORK
INVENTORS NAME: Selim Aissi et al.
DOCKET NO.: 884.830US1

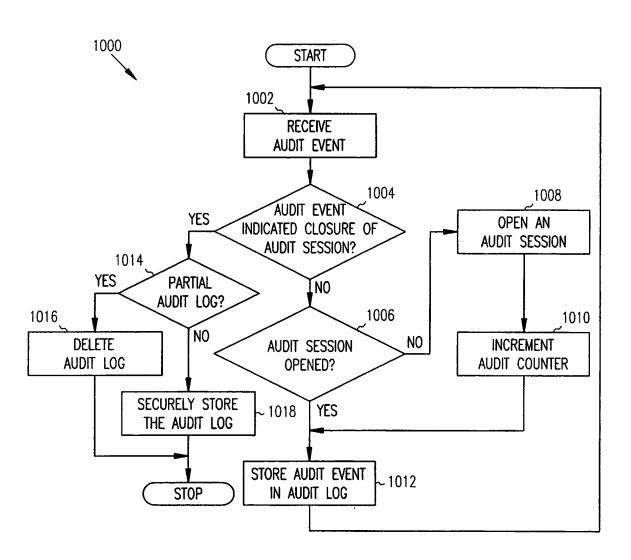11/11
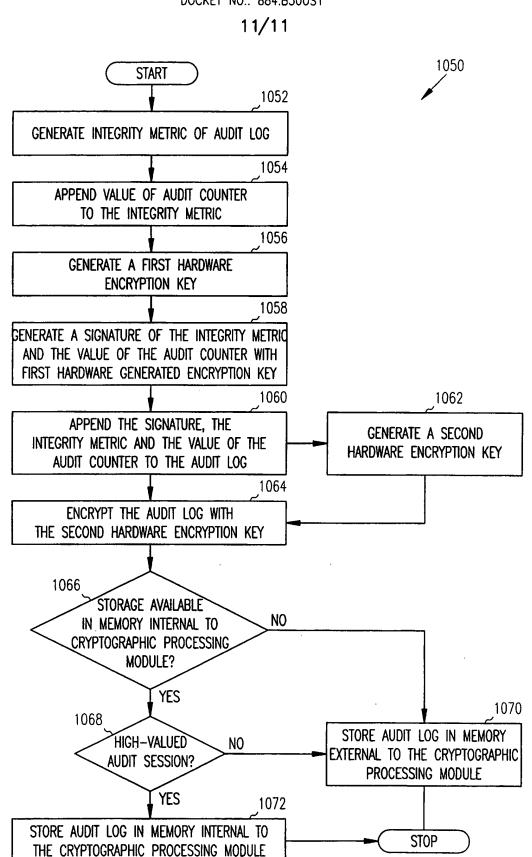
1050

START

GENERATE INTEGRITY METRIC OF AUDIT LOG — 1052

APPEND VALUE OF AUDIT COUNTER
TO THE INTEGRITY METRIC — 1054

GENERATE A FIRST HARDWARE
ENCRYPTION KEY — 1056

GENERATE A SIGNATURE OF THE INTEGRITY METRIC
AND THE VALUE OF THE AUDIT COUNTER WITH
FIRST HARDWARE GENERATED ENCRYPTION KEY — 1058

APPEND THE SIGNATURE, THE
INTEGRITY METRIC AND THE VALUE OF THE
AUDIT COUNTER TO THE AUDIT LOG — 1060

GENERATE A SECOND
HARDWARE ENCRYPTION KEY — 1062

ENCRYPT THE AUDIT LOG WITH
THE SECOND HARDWARE ENCRYPTION KEY — 1064

1066
STORAGE AVAILABLE
IN MEMORY INTERNAL TO
CRYPTOGRAPHIC PROCESSING
MODULE?

NO

YES

1068
HIGH-VALUED
AUDIT SESSION?

NO

STORE AUDIT LOG IN MEMORY
EXTERNAL TO THE CRYPTOGRAPHIC
PROCESSING MODULE — 1070

YES

STORE AUDIT LOG IN MEMORY INTERNAL TO
THE CRYPTOGRAPHIC PROCESSING MODULE — 1072

STOP

FIG. 10B